# THE EUROPEAN UNION'S GENERAL DATA PROTECTION REGULATION

BY: AUSTIN DENNY, PMG

pmg

# EXECUTIVE SUMMARY

## SCOPE

- Applies to any company processing personal data that results from EU-related transactions, regardless of the company's location.
- Companies in breach can be fined 4% of annual turnover or **20M EUROS**, whichever is greater.
- GDPR set to go into effect in the EU on **MAY 25, 2018**.
- Replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe.
- Regulations apply to both data controllers and processors in the EU and abroad.

## REQUIREMENTS

- Consent to the use of customer data **MUST** be collected via an intelligible and easily accessible form (no 'legalese' allowed). Equally important, the option to rescind consent must be just as easy to find/understand.
- Data subjects have the right to request of data processors confirmation as to whether and how their data is being used (Do you have my data? If so, why?). Processors must also provide a copy of personal data upon request.
- Data subjects have **THE RIGHT TO BE FORGOTTEN**, ceasing all dissemination of data and further use.
- Data subjects have the **RIGHT TO REQUEST** their data and to transfer it to another provider.
- Controllers and Processors whose core activities consist of processing operations will be required to hire data protection officers.
- **PRIVACY BY DESIGN** requires providers to structure their businesses and operations in such a way that supports the effective compliance with GDPR.

# AN IN-DEPTH INTRODUCTION TO GDPR

Over the last 15 years, we've witnessed the rise to dominance of aggregation-based services that have fundamentally altered the ways in which our global economy relies upon the use of personal data. An unavoidable reality in the age of Facebook and Google is the significant consolidation of users' digital activity and personal data, but their primary nature as tools for discovery has enabled the proliferation of personal data processing by smaller organizations propelled to success through vastly more efficient means of reaching their target markets.

Inevitably, the concept of natural rights and its corresponding regulatory protection has not kept pace with technical innovation in largely free markets. The EU's most recent regulation, Data Protection Directive 95/46/EC, was introduced in 1995 - only one year after internet protocols became commercially available. Now, 23 years later, the EU is poised to introduce its much-anticipated replacement, the General Data Protection Regulation (GDPR).

Mired in widespread confusion during its nearly six-year formulation period, GDPR's implementation is now only a short four months away. And while becoming completely compliant overnight is a near impossibility, for organizations that find themselves behind the times, we have two pieces of good news:

1.) The most critical requirements in GDPR can be achieved with relatively little technical debt and by setting reasonable milestones.

2.) Significant favor will be granted to organizations in the assessment of relative compliance that can demonstrate a general awareness of the regulation and an internal drive to become compliant.

To help illuminate the path to GDPR compliance, we've combed through the full GDPR text —with our digital marketing hat on—and have compiled some thoughts on what you absolutely need to know: GDPR's scope and applicability, its most pressing requirements, and how to think about your position as an organization.

But first, a disclaimer.

I'm not an attorney... not even close. Other than a few EU Law classes in business school, my interpretation of the GDPR is coming from an ad-tech product development perspective. That being said, I've seen a lot of blog posts and "thought-leadership" articles feigning legal wisdom on the subject that are just plain wrong. Please do not stake the liability of your organization on any publication (even this one). Hire qualified legal counsel, acquire some data security credentials, and read the GDPR for yourself. Short of those things, this is a decent starting point.

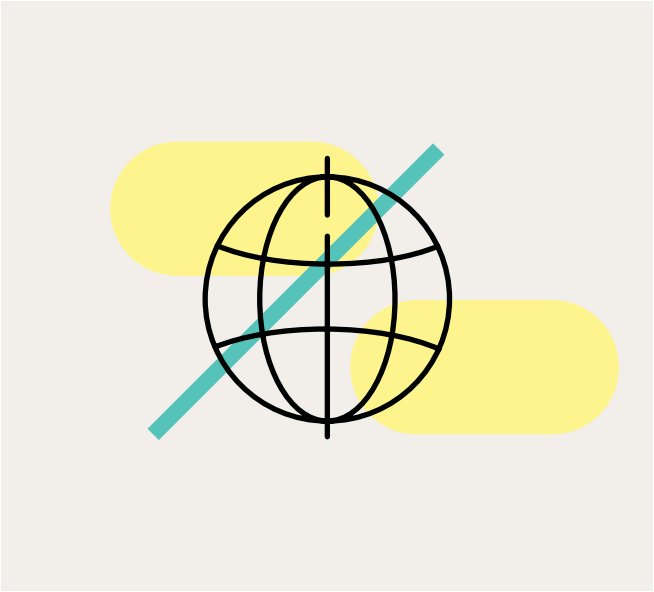
# THE GLOBAL SCOPE OF GDPR

MATERIAL VS. TERRITORIAL

## GLOBAL REACH

Perhaps the most perplexing aspect of GDPR in relation to how it will ultimately impact non-EU organizations is its considerably complex and broad assessment of jurisdiction and applicability. While many have made the argument that U.S.-based organizations and industries will remain fairly well insulated from the GDPR's regulatory reach, and have instead posited its implications in the U.S. as mere ideological diffusion, there are indeed no such geopolitical buffers to preclude any organizations from compliance.

The only cases in which organizations may violate the GDPR without consequence are those that meet two criteria: The offending organization does not maintain any EU-based operations, AND its host country is willing to block the enforcement of GDPR within its sovereign jurisdiction. However, it's not likely for this to ever be the case, particularly with regard to large organizations or serious GDPR offenses.



Rather, it's important to understand that, while GDPR is an EU regulation, it can potentially extend broad enforceability to non-EU organizations processing non-EU-person data. Thus, the need for compliance in post-industrialized digital societies outside of the EU is driven by both the general spread of consumer demand for privacy protection and potential real-world liability.

The GDPR achieves its status as a landmark stage in global privacy protection through Articles 2 & 3, which define material and territorial scope, respectively. Let's have a look at each concept individually to really understand how, when considered jointly, they manage such a broad reach.

## MATERIAL SCOPE

'Material' is a bit of a misnomer, as everything regulated by GDPR can be simplified down to electrons on a wire representing a series of zeros and ones. The material scope of GDPR refers to the actual data being processed. There are a few key pieces of the material scope that aren't immediately apparent when thinking about an EU law's protection of non-EU persons. The first is the concept of natural persons.

Recital 1 of GDPR states:

> *The protection of natural persons in relation to the processing of personal data is a fundamental right.*

It's on the very first page, so even if you get bored after two minutes of reading and give up, you'll at least see this part. The word 'European' is mentioned 13 times on the first page but does not appear in the first sentence of Recital 1, so you'd be forgiven for assuming that the material scope of protected data pertains singularly to EU persons.

Further, Article 2.1 states:

> *This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.*

Again, we see GDPR asserting applicability to all persons, not only EU persons. Subsequent provisions in Article 2 outline that the regulation does not apply in the course of an activity which falls outside the scope of Union law. All this means is that personal data captured during the rendering of goods and services outside of the Union are not regulated. It's most important here to note what is intentionally not mentioned: a narrowing definition of those protected to EU persons. When GDPR defines protection for **NATURAL PERSONS**, it refers to **ANY** person executing a transaction within the scope of Union law.

This should start to hint at why GDPR is so broad-reaching; any person undertaking a relevant activity in the EU can turn themselves into a protected data subject within a matter of minutes. And as we'll see, the second unexpected push of GDPR beyond the scope naturally conjured by the phrase 'European Union' is geographic in nature. The movement of a person's data internationally, their physical location, and the physical location of the organization controlling their data all play further in complicating and expanding roles regarding the applicability of GDPR.

## TERRITORIAL SCOPE

Fortunately, the GDPR is slightly more forthright in defining its territorial scope. Article 3 clearly illustrates its nature, summarized here as GDPR

- applies to processing personal data by an organization in the Union, regardless of where the processing takes place[1].
- applies to the processing of personal data of people who are in the Union (not just EU persons), as such data relates to[2]
    - the offering of goods or services (irrespective of required payment).

[1] Article 3.1
[2] Article 3.2.a-b

- the monitoring of their behavior that takes place in the Union.
- applies to the processing of personal data by an organization not established in the Union.

With territorial scope and Article 3 in mind, a cogent legal argument to make—that will surely make you the de-facto office expert (a title you definitely don't want, unless your job depends upon it)—is, "GDPR covers everything." When asked how, just respond, "because I say so." Sixty percent of the time, it works every time.

On the off chance it doesn't work, it helps to apply the scope to some practical examples. Yes, it's as fun as it sounds. Let's try one.

> You're part of a U.S.-based market research firm and are given a project of determining the relative product-attribute preferences of EU consumers with regard to a client's plan to develop a revolutionary vegetable-chopping device that will ultimately be sold in the EU. Your client hired a separate U.S.-based firm to conduct a survey of potential customers. A few weeks later, you receive the survey results which are all tied to households and individuals.

In this case, it doesn't matter that the client's location is undefined, or that both firms processing the market research data are located in the U.S. Because the data was collected from people physically in the EU, their data is subject to GDPR protection, meaning all companies involved in its processing need to be compliant.

## UNDERSTANDING YOUR ORGANIZATION'S ROLE

CONTROLLER VS. PROCESSOR

### WHO AM I?

Having mapped the applicability of GDPR to certain circumstances, we're still a bit lost without also understanding the true nature of our organizations and their relevant requirements.

In relation to their use of personal data, the GDPR classifies organizations as either controllers or processors. And as much as their labels entail—the GDPR is meant to be broadly understood—some organizations **CONTROL** the provenance, ultimate purpose, and protection of personal data, while other organizations **PROCESS** that data on behalf of controllers in joint pursuit of its ultimate purpose.

The strict definition of controllers and processors is pretty clearly outlined in Article 4, but naturally, some shades of gray arise with little additional consideration. Take PMG for example. We process hundreds of millions of customer records that constitute personal data on behalf of our clients. Under GDPR, we'd

overwhelmingly be considered a processor, but as a service provider, we also have customers and leads, about whom we maintain personal information. In that sense, despite the volume of data being orders of magnitude smaller than our processor operations, we are in fact also a controller. It's likely that most organizations will have some overlap.

## UNIQUE RESPONSIBILITIES OF CONTROLLERS

Articles 24 & 25 broadly enumerate the three primary things that controllers need to be aware of and work to build as a part of their operational workflow.

First, controllers are charged with defining what data processing really means in the context of their business. This definition is critical to get right; it's what will be included when asking users for consent, so keep it brief yet comprehensive, and descriptive yet succinct and comprehensible. With defined purposes in mind, controllers must then assess the possible associated risks and put the necessary safeguards in place.

> *Taking into account the nature, scope, context, and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure an to be able to demonstrate that processing is performed in accordance with this regulation.*[3]

If, as part of your processing of personal data, it's likely to be transmitted to multiple processors, a reasonable risk you face is the malicious interception or accidental dissemination of the data during transfer between parties. This could result from a mistake as simple as a junior employee sending unsecured personal data via email. Equally simple is the security control that would ensure GDPR compliance in such a situation: Only transfer personal data to authorized processors via encrypted channels that are subject to stringent access control (i.e., upload your customer data to an SFTP and only share the password with the single individual who needs access to enable processing).

Second, expanding this small example in a way that covers all potential situations, GDPR encourages controllers to pursue the concept of data protection by design and default. In other words, a practical implementation of technical and organizational mea-

[3] Article 24.1

sures to ensure that personal data is processed only to the reasonable extent of its purposes and is protected in storage and accessibility. A great way to achieve compliance in this field is through the preparation for and execution of a security audit (e.g., ISO 27001 security framework, SOC2 audit).

And third, they direct controllers to structure their general operations regarding personal data around a centralized code of conduct, the framework for which is generally outlined in Article 40.

### PROCESSORS AS EXTENSIONS OF CONTROLLERS

The obligations of processors, on the other hand, while being no less complex, are largely dictated by the needs and obligations of the controller. That is, when processing data on behalf of a controller, the processor must provide sufficient guarantees to implement technical and organizational measures to protect personal data at a level commensurate to that of the controller, i.e., in compliance with GDPR.[4]

The concept of equal levels of protection as data travels through a network of processors—think a person to a brand to a processor to an agency to another processor to a media network to an attribution partner or an analytics platform to a third processor and back to the brand—is not unique to the GDPR; it's currently baked into most data sharing contracts. However, in the context of GDPR, you can think of this as extending not only the data protection methods from controller to processor, but also as processing limitations based on the data's final purpose as defined by the controller.

## PRESSING REQUIREMENTS FOR DATA CONTROLLERS

The preceding 2,100 words, however tedious, are hopefully effective in their effort to make plain how the GDPR categorizes organizations within its purview and assesses the circumstances that may land an organization within its purview. Certainly, those are the most egregious points of confusion that the EU has kindly left up to us to make sense of.

They do not, however, do you much good when it comes to understanding the basic things your organization needs to do in the likely event that you are found to be within the enforceable jurisdiction of GDPR. Luckily, the EU threw us a bone on this part and compiled a decent breakout of the GDPR's most significant deviations from previous regulatory requirements. It can be found here, on the GDPR website, a recommended resource for those hoping to learn more.

#### ASIDE

I found the super cool doomsday clock on the home page notable, counting by the second down

[3] Article 28.1

to GDPR implementation, circa 2001 web-design standards. Also, pay attention to their disclaimer in the footer. You've now been given two disclaimers (and this is kind of a third). Seriously, hire a lawyer. I know it's expensive. Please do it. Please.

**/ASIDE**

All of the rights ensured by GDPR are generally described on the site and, in much greater detail, within the full text itself (which you're going to read after hiring a lawyer, right?), so I won't recount the basics ad nauseum here. Rather, let's think through what they mean in practical terms and some of the idiosyncratic requirements that make them unique from the old way of doing things, i.e., however we wanted with no oversight.

Broadly speaking, I think this section of GDPR divides itself nicely into two main areas: consent, and ensuring rights.

## GAINING CONSENT

Consent is the centerpiece of GDPR. Without a rigid model for defining what constitutes consent, all other aspects of the regulation fall apart. The murkiness of consent under previous regulations is the root cause of their failure to be understood and their broad abdication of enforcement activities.

Thus, consent under GDPR features some user-friendly bells and whistles. Most notable is the idea that consent is no longer implied through the use of a product or service.[5] If I visit your site, and you require that I log in with personal data, the simple act of my logging in will no longer constitute consent to the use of my personal data. The move from implied to explicit consent, of course, requires some updates to the mechanics of brand-customer interaction.

Controllers will have to come right out and ask customers—using plain, intelligible language—for their permission to collect and use personal data. In addition, the requirement that, in requesting consent, controllers must lay out all planned use cases for the processing of personal data implies that the processing scope must be narrow enough to provide for the

[5] Recitation 32

simple conveyance of the purposes contained within.

Now, a lot of companies out there already seek some level of consent from their users, so reaching compliance may only mean changing minor aspects of that process. In that sense, this requirement is perhaps not that groundbreaking. Far fewer, though—and this is based only on my personal experience—provide users with an equally accessible method for revoking consent… because, of course, why would we (collective we) do something so patently absurd?!

Take note, **ANY PERSON COVERED BY THE GDPR HAS THE RIGHT TO WITHDRAW HIS OR HER CONSENT AT ANY TIME, AND IT MUST BE AS EASY TO WITHDRAW CONSENT AS IT WAS TO GIVE IT**. We don't yet have a precedent for how this will be enforced, but the language reads to me like this:

> If a website gains consent from its users via a popup modal with big red text outlining all future uses of the user's personal data, every time a user re-authenticates on that site, they must again be served a big popup modal offering the right to revoke consent.

This is probably an overly simplistic example that relies on the slim chance that the future legal definition of equivalent ease in withdrawal will require the same step-by-step process. Nonetheless, I think we can assume that Facebook's desire to hide account deactivation—and, soon, consent withdrawal—several layers deep within a convoluted preferences menu tree as nondescript, greyed-out, non-underlined links won't be permitted under GDPR.

I can't overstate how critical this aspect of GDPR compliance is. If consent is gained or retained improperly, all subsequent activities will be assessed as non-compliant, which, simply put, would be bad. These changes are generally terrible news for many players in the digital advertising industry, aside from the dominant aggregators, but that's another article entirely (though likely not as lengthy).

## ENSURING FUNDAMENTAL RIGHTS

So, we've covered a lot, but haven't even touched on the major updates to the rights afforded to regular people, arguably the most important aspect of GDPR. Unfortunately, a lot of the time spent trying to understand GDPR is dedicated to the aspects of scope and applicability, which should ideally be simple, but tend to dominate internal planning discussions.

With that out of the way, though, here are the fundamental rights protected by the GDPR and what they generally mean in terms of preparation.

### RIGHT TO ACCESS

After gaining consent from a customer or user, controllers will be required to make whatever personal data they hold available to the subjects of that data. So, the first step in this process is to enable a system that both verifies the identity of the person making the request and subsequently confirms whether their personal data are being used.

If the presence of said data is confirmed, the controller must also make it available to its respective human in a format easily read by a computer, i.e., JSON, XML, etc. There's no telling how frequently this right will be exercised, which I imagine will dictate the best solution, whether that's programmatic or managed by real people in the more traditional practice of customer service.

### RIGHT TO BE FORGOTTEN

This is pretty simple. Should someone confirm with a controller that their data is being processed, they then, in addition to requesting a copy of the data, have the right to instruct the controller to purge their personal data, effectively causing them to be "forgotten." In terms of operations, this could pretty easily rest on the shoulders of whatever process is implemented to ensure compliance with the right to access.

### RIGHT TO DATA PORTABILITY

Currently, if you request your historical personal data from Facebook, to include site behavior, it comes—if not pulled via their poorly documented API—in the form of a PDF. There's a reason for this, and if you took a curious note of the requirement for computer readability within the right to access, you might have an idea of where this is going.

Personal data has historically been viewed by advertising-reliant platforms as a valuable commodity, one which should be protected from competitors. Earlier I mentioned that the GDPR seeks to shift the power over personal data from large organizations to the people themselves, and this is perhaps the most significant provision in that effort. Despite the incentives for companies to obscure and protect the personal data they process, the right to data portability states that, after receiving a computer-readable copy of their data, users may transfer that data freely to any other controller they see fit.

I'm doubtful that new option this will materialize into any kind of mass chaos or a real threat to the established platforms that hold the majority of personal information, but it is an interesting factor in the assessment of switching costs for customers considering new entrants in any industry.

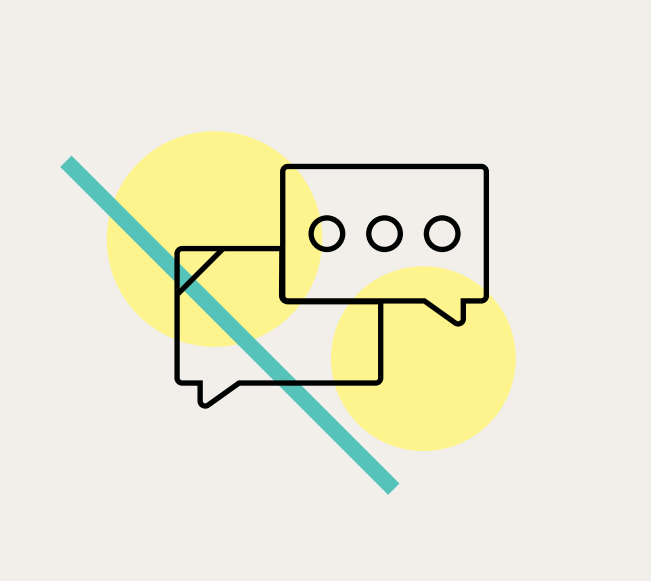
### RIGHT TO OBJECTION

An important piece, this is. Currently, there are some consumer protections regarding the necessary consent for personal data to be used in the pursuit of direct marketing goals. However, the application and

clarity of companies' compliance is muddy at best. What the right to objection states is, if a person determines that a company processes their personal data, they may allow the company to retain their data for the purposes of rendering a product or service, but may disallow the company from using their data in any way for marketing purposes. This includes the use of their personal data in the broader analysis of customer cohorts, or any similar profiling activity.

## OTHER AREAS OF INTEREST

At this point, you hopefully have a good mental model with which to assess your organization's position and responsibilities relative to the GDPR. And while that's more than half of the battle, this is not a comprehensive analysis.



Beyond the initial scope and effects of the regulation, other aspects we intend to explore further are the rights of the data subjects (private citizens), how GDPR will affect advertisers, and the incongruencies between the future of digital privacy and the overarching economics of the internet. In each of these areas—and I'm sure in other tangentially related topics that haven't yet crossed my mind in this context—there are interesting developments and trade-offs happening daily which will have long-lasting effects on our industry. Taking a step back from the daily grind to consider these macro elements will help all of us to position our organizations for success in the future… and also subsequent articles should be much more interesting and definitely shorter.

Lastly, hire a lawyer.

---

Austin Denny leads PMG's global audience practices, directing customer research, media targeting strategy, and the development of our deterministic audience platform. He is not a lawyer.